

1 This listing of claims will replace all prior versions, and listings, of claims
2 in the application:

3

4 **Listing of Claims**

5

6 Claim 1 (Currently amended): A method for accommodating a legacy
7 application, the legacy application resident on a legacy system having provisions
8 for a low-level credential authorization model which employs username-and-
9 password based authorization, the method comprising:

10 obtaining a request from a high-level credential authorization model for a
11 high-level credential to be provided by the legacy application, wherein the high-
12 level credential authorization model does not employ username-and-password
13 based authorization; [[and]];

14 retrieving the requested high level credential from a database of credentials;
15 and

16 marshaling the requested high-level credential, the marshaling is
17 characterized by converting a description of the high-level credential into a format
18 recognizable as a low-level credential by the legacy application employing a low-
19 level credential authorization model, wherein the marshaling is a mechanism by a
20 which a description of the high-level credential is passed through a secured
21 operating system layer using an interface designed to output low-level credentials.

22

23 Claim 2 (Original): A method as recited in claim 1 further
24 comprising, after the obtaining, seeking the requested credential in a database of
25 credentials.

1
2 Claim 3 (Original): A method as recited in claim 1, wherein a high-
3 level credential is a credential selected from a group composed of X.509
4 Certificates and bio-metrics.

5
6 Claim 4 (Original): A method as recited in claim 1, wherein the
7 marshaled credentials appear to be a conventional username/password pair to the
8 legacy application.

9
10 Claim 5 (Previously presented): A method as recited in claim 1, wherein
11 marshaling comprises:

12 obtaining the requested high-level credential;
13 converting the requested high-level credential to generate a low-level
14 credential that represents the requested high-level credential while appearing to be
15 a conventional username/password pair to the legacy application.

16
17 Claim 6 (Original): A method as recited in claim 1, wherein the
18 legacy application never has access to the high-level credential.

19
20 Claim 7 (Original): A computer-readable medium having computer-
21 executable instructions that, when executed by a computer, perform a method as
22 recited in claim 1.

1 Claim 8 (Currently amended): In a computing environment where
2 certain processes have a provision for low-level credentials but have no provision
3 for high-level credentials, wherein a provision for low-level credentials employs
4 username-and-password based authorization while a provision for high-level
5 credentials does not employ username-and-password based authorization, a
6 method for accommodating such processes comprising:

7 obtaining a request for a credential from a process, wherein the requested
8 credential is a high-level credential, which is not username-and-password based;

9 retrieving the requested credential from a database;

10 converting the requested high-level credential into a format approximating a
11 low-level credential and representative of the requested high-level credential; and

12 returning the converted credential to the process

13 passing a description of the high-level credential through a secured
14 operating system layer using an interface designed to output low-level credentials.

15

16 Claim 9 (Original): A method as recited in claim 8, wherein a high-
17 level credential is a credential selected from a group composed of X.509
18 Certificates and bio-metrics.

19

20 Claim 10 (Original): A method as recited in claim 8, wherein the
21 converted credentials appear to be a conventional username/password pair to the
22 process.

23

24 Claim 11 (Original): A method as recited in claim 8, wherein the
25 process never has access to the high-level credential.

1

2 Claim 12 (Original): A computer-readable medium having computer-
3 executable instructions that, when executed by a computer, perform a method as
4 recited in claim 8.

5

6 Claim 13 (Currently amended): A method for authenticating a
7 user to a network, the method comprising:

8 obtaining a request for a high-level credential to authenticate the user to
9 access a resource within the network, wherein the resource requires an appropriate
10 high-level credential before the user may access the resource;

11 locating the appropriate high-level credential;

12 passing a description of the high-level credential, in place of the low-level
13 credential, through a secured operating system layer using an interface designed to
14 output low-level credentials.

15 returning the appropriate high-level credential to the resource within the
16 network, so that the resource allows the user to access such resource;

17 wherein the obtaining, locating, [[and]] returning, and passing are
18 performed without user interaction so that the user need not be aware that such
19 steps are being performed.

20

21 Claim 14 (Original): A method as recited in claim 13 further
22 comprising repeating the obtaining, locating, and returning for a different network
23 that is authenticated using a different credential.

24

25

1 Claim 15 (Original): A computer-readable medium having computer-
2 executable instructions that, when executed by a computer, perform a method as
3 recited in claim 13.

4

5 Claims 16-17 (Canceled)

6

7 Claim 18 (Currently amended): A credential management architecture,
8 comprising:

9 a trusted computing base (TCB) that has full access to persisted credentials,
10 the TCB being configured to interact with an untrusted computing layer (UTCL)
11 that accesses the persisted credentials via the TCB,

12 the TCB comprises:

13 a credential management module configured to receive requests from
14 the UTCL for a high-level credential for a resource, the high-level
15 credential being associated with a user and not being username-and-
16 password based authorization;

17 a credential database associated with the user, wherein credentials
18 are persisted within the database;

19 the credential management module being configured to retrieve
20 credentials from the database; and

21 an interface for passing a description of a high-level credential, in
22 place of the low-level credential, designed to output low-level credentials,

1 Claim 19 (Previously presented): An architecture as recited in claim
2 18, wherein credential management module is further configured to marshal a
3 requested high-level credential and return the marshaled credential to the UTCL.

4

5 Claim 20 (Original): An architecture as recited in claim 18, wherein
6 the marshaled credentials appear to be a conventional username/password pair to
7 the UTCL.

8

9 Claim 21 (Original): A computer-readable medium having computer-
10 executable instructions that, when executed by a computer, employ an architecture
11 as recited in claim 18.

12

13 Claim 22 (Original): An operating system embodied on a computer-
14 readable medium having computer-executable instructions that, when executed by
15 a computer, employ an architecture as recited in claim 18.

16

17 Claim 23 (Currently amended): An apparatus comprising:
18 a processor;
19 a marshaler executable on the processor to:

20 obtain a high-level credential, wherein a high-level credential
21 is employed in an authorization model which is not username-and-
22 password based authorization;

23 convert the high-level credential to generate a representation
24 of the high-level credential that is formatted as a low-level credential
25 so that it appears to be a conventional username/password pair; and

pass a description of the high-level credential through a secured operating system layer using an interface designed to output low-level credentials.

Claim 24 (Currently amended): An accommodation system comprising:
a request obtainer configured to obtain a request for a high-level credential
from a low-level-credential-application, wherein low-level credentials utilizes
username-and-password based authorization while high-level credentials do not
employ username-and-password based authorization;

a credential retriever configured to retrieve the requested credential from a database of credentials;

a marshaler configured to marshal the requested credential and return the marshaled credential to the low-level-credential-application, wherein marshaling performed by the marshaler is characterized by converting a description of the high-level credential into a format recognizable as a low-level credential by the low-level-credential-application employing a low-level credential authorization model and passing a description of the high-level credential through a secured operating system layer using an interface designed to output low-level credentials.

Claim 25 (Original): A system as recited in claim 24, wherein a high-level credential is a credential selected from a group composed of X.509 Certificates and bio-metrics.

1 Claim 26 (Original): A system as recited in claim 24, wherein the
2 marshaled credentials appear to be a conventional username/password pair to the
3 legacy application.

4

5 Claim 27 (Canceled)

6

7 Claim 28 (Previously presented): A system as recited in claim 24, wherein
8 the low-level-credential-application never has access to the high-level credential.

9

10 Claim 29 (Currently amended): A system for authenticating a user to a
11 network, the system comprising:

12 a request obtainer configured to obtain a request for a high-level credential
13 to authenticate the user to access a resource within the network, wherein the
14 resource requires an appropriate credential before the user may access the
15 resource, wherein a high-level credential do not utilize username-and-password
16 based for high-level credential authorization;

17 a credential retriever configured to retrieve the appropriate high-level
18 credential from a database of credentials;

19 a credential marshaler configured to generate a representation of the high-
20 level credential formatted as a low-level credential so that it appears to be a
21 conventional username/password pair to a low-level-credential-application,
22 wherein a low-level credential utilizes username-and-password based
23 authorization, and pass a description of the high-level credential through a secured
24 operating system layer using an interface designed to output low-level credentials;
25 and.

1 a credential returner configured to return the marshaled high-level
2 credential to the resource within the network, so that the resource allows the user
3 to access such resource;

4 wherein the obtainer, retriever, marshaler, and returner are further
5 configured to operate without user interaction.

6
7 Claim 30 (Original): An operating system comprising a system as
8 recited in claim 29.

9
10 Claim 31 (Original): A network environment comprising a system as
11 recited in claim 29.

12
13 Claim 32 (Currently amended): An application programming interface
14 (API) method comprising:

15 receiving a CredUI-promptfor-credentials call having a set of parameters
16 comprising a TargetName, Context, AuthFlags, and Flags;

17 retrieving the parameters from the call to determine a specified resource;

18 obtaining a high-level credential;

19 associating the high-level credential with the specified resource;

20 persisting the high-level credential into a database while maintaining the
21 credential's association with the specified resource; and

22 passing a description of a high-level credential, in place of the low-level
23 credential, through a secured operating system layer using an interface designed to
24 output low-level credentials.

1 Claim 33 (Original): A method as recited in claim 32, wherein the set
2 of parameters further comprises an indicator of a data structure containing
3 customized information to display in conjunction with a user interface.

4

5 Claim 34 (Currently amended): An application programming interface
6 (API) method comprising:

7 receiving a CredUI-promptfor-credentials call having a set of parameters
8 comprising a TargetName, UserName, Password, and Flags;

9 retrieving parsing the call to retrieve the parameters from the call to
10 determine a requesting application;

11 obtaining a low-level credential from a user, wherein such credential
12 includes a username and a password; and

13 passing a description of a high-level credential, in place of the low-level
14 credential, through a secured operating system layer using an interface designed to
15 output low-level credentials.

16 returning the low level credential to the requesting application.

17

18 Claim 35 (Original): A method as recited in claim 34, wherein the set
19 of parameters further comprises an indicator of a data structure containing
20 customized information to display in conjunction with a user interface.

21

22 Claim 36 (New): A method as recited in claim 1, wherein the marshaling
23 is performed by creating a reference to a certificate by taking a certificate hash and
24 computing a text string for the certificate hash.

1 Claim 37 (New): A method as recited in claim 1, wherein the marshaling
2 is performed by creating a reference to credential stored in credential manager.
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25